UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,202	10/16/2001	Marc Charbonneau	12-69 US	3583

25319 7590 08/02/2006

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/977,202	CHARBONNEAU, MARC	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to remarks filed on 24, May 2006. Presently pending claims are 1 – 23.

Claim Rejections - 35 USC § 112

2. Applicant's arguments see Page 7, filed May 24, 2006, with respect to Claims 5 and 6 have been fully considered and are persuasive. In view of the amendments to the Claims 5 and 6, the 35 USC 112 rejection of Claims 5 and 6 has been withdrawn.

Response to Arguments

3. Applicant's arguments filed May 18, 2006 have been fully considered but they are not persuasive.

Bellemore et al. (U.S. Patent Number 5,944,825) teaches a method for providing security and password mechanisms in a data base system. The method limits access to the database to clients who transmit a valid password and user ID (authentication) combination. Furthermore, the method requires that passwords are changed periodically. The method ensures that passwords meet certain criteria.

Novoa et al. (U.S. Patent Number 6,636,973) teaches a server computer that dynamically changes a user's password and that the server computer uses a database that contains a password and biometric template value associated with each user.

Regarding claims 1 – 7, 11 and 18 - 21, Applicant argues that Bellemore does not teach, "a password database or other than the password database for storing a new password or data indicative of the new password and associating same with authentication data for the user", see Remarks page 10. These arguments are not found persuasive. Bellemore discloses, "From time to time, the security and password mechanisms require changing the password associated with a user ID (authentication data for the user) and the database management system updates the new password" (Column 4 lines 33 – 42). Furthermore, Bellemore discloses, user table, user profile table and user history table are updated with the new password along with the associated information (Column 4 line 45 – Column 5 line 41). Thus Bellemore discloses "a password database or other than the password database for storing a new password or data indicative of the new password and associating same with authentication data for the user".

Regarding claims 1, 5, 7 and 20, Applicant argues that Bellemore does not teach, "stores data indicative of the new password in a database other than the password database for later retrieval, the data indicative of the new password for use in providing the new password to the system automatically", see Remarks page 10. These

arguments are not found persuasive. Bellemore discloses, "user_name filed containing user-ID, account_status and login_attempts" (data indicative of the new password) reflecting the changes with password. Furthermore, Bellemore discloses that any or all of these data indicative of the new password will then be used by the system automatically to authenticate a user (Column 5 line 1 – 38). Thus Bellemore discloses, "stores data indicative of the new password in a database other than the password database for later retrieval, the data indicative of the new password for use in providing the new password to the system automatically".

Regarding claims 8 – 10, 12 – 15, 16 – 17 and 22 – 23, Applicant argues that admitted prior arts do not teach "performing an operation to change a password of the known user to a new password in the system automatically" and "storing the new password in a database independent of the change password operation and other than the password database where the changed password is stored by the change password operation", see Remarks page 11. These arguments are not found persuasive. Bellemore discloses changing the password associated with the a user ID (Column 5 lines 1 – 38) and Novoa discloses dynamically and automatically changing the password (Novoa Column 7 lines 8 – 28 and Column 8 lines 39 – 54). Bellemore discloses, "user_name filed containing user-ID, account_status and login_attempts" (data indicative of the new password) reflecting the changes with password. Furthermore, Bellemore discloses that any or all of these data indicative of the new

password will then be used by the system automatically to authenticate a user (Column 5 lines 1 – 38).

Thus Bellemore in view of Novoa discloses, "performing an operation to change a password of the known user to a new password in the system automatically" and Bellemore discloses, "storing the new password in a database independent of the change password operation and other than the password database where the changed password is stored by the change password operation".

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "a password database or other than the password database for storing a new password or data indicative of the new password and associating same with authentication data for the user" and "stores data indicative of the new password in a database other than the password database for later retrieval, the data indicative of the new password for use in providing the new password to the system automatically", broadly recited in the independent claims 1, 7 and 20. The dependent claims 2 – 6, 8 – 19 and 21 – 23 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending claims 1 –23 is respectfully maintained.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1 – 7, 11, 18 – 20 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Bellemore et al. (U.S. Patent Number 5,944,825, hereinafter "Bell").

Regarding Claim 1, Bell teaches detecting an occurrence of a password change operation in execution on a system having a password database that stores passwords resulting from a password change operation (Bell Column 4 lines 5 – 37 and Column 9 lines 2 – 30);

detecting a new password when provided (Bell Column 4 lines 33 – 40); and,

storing data indicative of the new password in a database other than the password database for later retrieval, the data indicative of the new password for use in providing the new password provision to the system automatically (Bell Column 4 lines 33 – 42 and Column 6 line 66 – Column 7 line 16).

Regarding Claim 5, Bell teaches detecting a change password operation in execution on a system for changing a first password, the system having a password database that stores said first password (Bell Column 4 lines 5 – 37 and Column 9 lines 2 – 30);

displaying to a user a prompt for a new password in response to detecting the change password operation in execution and other than occurring as an operation of the change password operation (Bell Column 3 lines 29 – 52 and Column 4 lines 33 – 40);

receiving the new password (Bell Column 4 lines 33 – 40);

performing an operation to change the password to the new password in the system (Bell Column 4 lines 33 – 40 and Column 6 lines 1 – 22); and,

storing the new password in a database independent of the change password operation and independent of the password database where at least the changed password is stored by the change password operation (Bell Column 6 lines 11 – 36).

Regarding Claim 7, Bell teaches detecting a password change operation in execution on a system having a password database that stores passwords resulting from a password change operation (Column 4 lines 5 – 37);

displaying to a user a prompt for authentication information in response to detecting the change password operation in execution and other than occurring as an operation of the change password operation (Bell Column 3 lines 29 – 52 and Column 4 lines 33 – 40);

receiving the authentication information (Bell Column 4 lines 20 – 33 and Column 5 lines 47 – 53);

when the authentication information is indicative of a known user, performing an

operation to change the password of the known user to a new password in the system (Bell Column 4 lines 33 – 42; Column 5 lines 54- 59 and Column 6 line 66 – Column 7 line 13); and,

storing the new password in a database independent of the change password operation and independent of the password database where the changed password is stored by the change password operation (Bell Column 6 lines 11 – 36 and Column 7 lines 4 – 19).

Regarding Claim 20, Bell teaches detecting a password change operation in execution on a system having a known user authorized thereon (Bell Column 4 lines 5 – 37);

automatically generating a new password in response to detecting the password change operation and other than occurring as an operation of the change password operation and storing the new password in a password database (Bell Column 1 lines 11 – 34 and Column 7 lines 4 – 19);

performing an operation to change the password to a new password in the system (Bell Column 4 lines 33 – 42; Column 5 lines 54- 59 and Column 6 line 66 – Column 7 line 13); and,

storing the new password in a database independent of the change password operation and of the password database where the changed password is stored (Bell Column 6 lines 11 – 36 and Column 7 lines 4 – 19).

Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein detecting an occurrence of a change of password operating in execution on a system comprises detecting a new password prompt (Bell Column 4 lines 33 – 37)

Claim 3 is rejected applied as above in rejecting Claim 1. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), comprising the steps of:

prompting a user to provide authorization data, the authorization data being other than the new password (Bell Column 2 lines 34 – 41 and Column 4 lines 33 – 37); and

associating the authorization data with the new password (Bell Column 2 lines 34 – 59; Column 4 lines 20 – 42 and Column 7 lines 4 –19).

Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein detecting the new password comprises detecting the new password at least two separate times (Bell Column 3 line 56 – Column 4 line 42).

Claim 6 is rejected applied as above in rejecting Claim 5. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein detecting the change password operation in execution on a system comprises detecting password change command operations (Bell Column 4 line 33 – 37).

Claim 11 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein performing an operation to change the password comprises providing the new password to the system (Bell Column 7 lines 5 – 19).

Claim 18 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), comprising performing another operation to change another password of known user to the new password (Bell Column 7 lines 5 – 19).

Claim 19 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), comprising:

determining within the password database and associated with a same user all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password (Bell Column 8 line 46 – Column 9 line 9).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 8 – 10 and 12 – 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellemore et al. (U.S. Patent Number 5,944,825, hereinafter "Bell") in view of Novoa et al. (U.S. Patent Number 6,636,973, hereinafter "Novoa").

Claim 8 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), prompt for authentication information (Bell Column 4 lines 5 – 37). Bell does not teach that the prompt for authentication information is a prompt for biometric information. However, Novoa discloses a biometrics-based password change method for securely changing password includes prompting for authentication information wherein authentication information a prompt for biometric information (Column 4 lines 40 – 63 and Column 5 lines 3 – 43).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Novoa's biometric-based password change method into the securely password changing method of Belle's.

Bell could have been modified by Novoa to arrive at the claimed invention by having the database, security process that are adapted for monitoring and detecting the password change request to request for the authentication information (Bell Column 4 lines 5 – 37) to be biometric information as taught by Novoa (Novoa Column 2 lines 27 – 41 and Column 6 lines 3 – 26). One of ordinary skill in the art would have been motivated to modify Bell by Novoa as discussed above because in a password based system, an unauthorized person who is able to obtain a valid password can still access the system while in a biometric-based system, the user needs both password and biometric information to access the system, thus using biometric authentication information would increase and improve network and system security as taught by Novoa.

Claim 9 is rejected applied as above in rejecting Claim 8. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), comprising:

providing biometric information (Novoa Column 4 lines 59 – 61 and Column 6 lines 27 – 41);

processing the provided biometric information to provide the biometric data (Novoa Column 6 lines 67 – Column 7 line 65);

comparing the biometric data with a stored template (Novoa Column 7 lines 36 – 65); and

in dependence upon a comparison result retrieving a user password from a database (Novoa Column 7 line 36 – Column 8 line 10).

Claim 10 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein the prompt for authentication information prompt for information relating to data stored in a memory of a smart card (Novoa Column 7 lines 29 – 35).

Claim 12 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein performing an operation to change the password comprises prompting the user to select between provision of the new password and automatic generation of the new password (Novoa Column 7 lines 1 – 10 and lines 39 – 54).

Claim 14 is rejected applied as above in rejecting Claim 7. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein performing an

operation to change the password comprises automatically generation of the new password (Novoa Column 7 lines 1 – 10 and lines 39 – 54).

Claims 15 and 21 are rejected applied as above in rejecting Claims 13 and 20. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein the automatically generated new password is unknown to the user (Novoa Column 7 lines 1 – 10 and lines 39 – 54).

Claim 13 is rejected applied as above in rejecting Claim 12. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein performing an operation to change the password comprises automatically generation of the new password (Novoa Column 7 lines 1 – 10 and lines 39 – 54).

6. Claims 16, 17, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellemore et al. (U.S. Patent Number 5,944,825, hereinafter "Bell") in view of Novoa et al. (U.S. Patent Number 6,636,973, hereinafter "Novoa") further in view of Schneier (Bruce Schneier "Applied Cryptography, Second edition; hereinafter "Schneier").

Claims 16 and 22 are rejected applied as above in rejecting Claims 15 and 21. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5; Summary and Column 3 line 29 – Column 7 line 19), wherein the automatically generated new password is an encryption key (Bell Column 7 lines 5 – 19 and Novoa Column 7 lines 1 – 10 and lines 39 – 54 and Column 8 lines 11 – 18). Bell discloses securely changing password and Novoa discloses automatically generating new password. Even when taken together, Bell and Novoa do not disclose that the newly generated password is an encryption key. However, Schneier teaches that the passwords that are generated using randomly as taught by Novoa can be used as encryption keys (Schneier Pages 173 and 174). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Novoa's biometric-based password change method into the securely password changing method of Belle's and to use the automatically generated password as an encryption key.

Bell could have been modified by Novoa to arrive at the claimed invention by having the database, security process that are adapted for monitoring and detecting the password change request to request for the authentication information (Bell Column 4 lines 5 – 37) to be biometric information as taught by Novoa (Novoa Column 2 lines 27 – 41 and Column 6 lines 3 – 26) wherein the password is an encryption as taught by Schneier. One of ordinary skill in the art would have been motivated to modify Bell by Novoa and Schneier as discussed above because in a password based system, an unauthorized person who is able to obtain a valid password can still access the system

while in a biometric-based system, the user needs both password and biometric information to access the system, thus using biometric authentication information would increase and improve network and system security as taught by Novoa wherein the password is an encryption key, as taught by Schneier.

Claims 17 and 23 are rejected applied as above in rejecting Claims 16 and 22. Furthermore, Bell teaches and describes a method of securely supporting password change (Bell Fig. 1 – 5, Summary and Column 3 line 29 – Column 7 line 19) Bell discloses securely changing password and Novoa discloses automatically generating new password (Bell Column 7 lines 5 – 19 and Novoa Column 7 lines 1 – 10 and lines 39 – 54 and Column 8 lines 11 – 18). Even when taken together, Bell and Novoa do not disclose that the new password is encrypted using the encryption key. However, Schneier teaches that the new password is encrypted using the encryption key (Schneier Page 173 and 174). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Novoa's biometric-based password change method into the securely password changing method of Belle's and to encrypt the password using an encryption key to provide secure password.

Bell could have been modified by Novoa to arrive at the claimed invention by having the database, security process that are adapted for monitoring and detecting the password change request to request for the authentication information (Bell Column 4 lines 5 – 37) to be biometric information as taught by Novoa (Novoa Column 2 lines 27 – 41 and Column 6 lines 3 – 26) wherein the password is encrypted using the

encryption key as taught by Schneier. One of ordinary skill in the art would have been motivated to modify Bell by Novoa and Schneier as discussed above because in a password based system, an unauthorized person who is able to obtain a valid password can still access the system while in a biometric-based system, the user needs both password and biometric information to access the system, thus using biometric authentication information would increase and improve network and system security as taught by Novoa wherein the password is encrypted using the encryption key which is difficult to decrypt without the key, as taught by Schneier.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to

the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
July 24, 2006.

NASSER MOAZZAMI
PRIMARY EXAMINER

7,28,06